UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/980,582	04/04/2002	Steve Vestergaard	D383 0001/TAR	5988

720 7590 07/13/2007

OYEN, WIGGS, GREEN & MUTALA LLP
480 - THE STATION
601 WEST CORDOVA STREET
VANCOUVER, BC V6B 1G1
CANADA

EXAMINER	
TO, BAOTRAN N	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
07/13/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/980,582	VESTERGAARD ET AL.	
	Examiner	Art Unit	
	Baotran N. To	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04/30/2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6,11,17,18,20,21,25,27,28,31,33-36,38,40-44 and 46-56* is/are pending in the application.

4a) Of the above claim(s) *See Continuation Sheet* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6,11,17,18,20,21,25,27,28,31,33-36,38,40-44 and 46-56* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Continuation of Disposition of Claims: Claims withdrawn from consideration are 7-10,12-16,19,22-24,26,29-30,32,37,39 and 45 (canceled).

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 04/30/2007 has been entered.

This Office Action responds to the Applicant's Amendment filed 04/30/2007.

Claims 21, 25, 41, 47-48 and 51-52 are amended.

Claims 7-10, 12-16, 19, 22-24, 26, 29-30, 32, 37, 39 and 45 are cancelled.

Claims 55-56 are newly added.

Claims 1-6, 11, 17, 18, 20, 21, 25, 27, 28, 31, 33-36, 38, 40-44 and 46-56 remain for examination.

Response to Arguments

2. Applicant's arguments with respect to Claims 1-6, 11, 17, 18, 20, 21, 25, 27, 28, 31, 33-36, 38, 40-44 and 46-56 have been considered but are moot in view of the new ground(s) of rejection Eberhard et al. (U.S. Patent Publication 2001/001238 A1) herein referred to as Eberhard.

Applicant argues, "The Examiner appears to express the view, on page 3 of the Office Action, that the En-Seung et al. 'temporary validation key" exhibits the characteristics of the claim 1 'decryption key' and that the En-Seung et al. 'user's key' exhibits the characteristics of the claim 1 'user key'. With respect, the Applicant submits that this view is incorrect."

Examiner respectfully disagrees with applicant. En-Seung clearly discloses the step of "receiving the decryption key from the remote server at the user computing device, the decryption key itself encrypted at the remote server with a user key such as "Service server 12 generates the header with the user's authorization information including the temporary validation key that has been encrypted wit the user's key. Service server 12 then adds the encrypted digital information to the header in order to generate the protocol for copyright protection. The protocol for copyright protection is transmitted to the user's terminal unit 10 through the network (col. 3, lines 30-36).

For at least the above reasons, En-Seung reference is maintained.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 3, 17, 21, 25, 36, 38, 14-39, 41-42, 46-50 and 55 are rejected under 35 U.S.C. 103(a) as being unpatentable over Glover (U.S. Patent 6,052,780) herein referred to as Glover in view of En-Seung et al. (U.S. Patent 6,892,306 B1) herein referred to as En-Seung and further in view of Eberhard et al. (U.S. Patent Publication 2001/001238 A1) herein referred to as Eberhard.

Regarding Claims 1 and 46, Glover discloses a method of distributing electronic media, the method comprising:

receiving a file (computer program) (col. 4, lines 30-35) at a user computing device,

the file comprising an integral decryption engine (decryption program) and encrypted media content (encrypted digital information) (col. 3, lines 45-50 and col. 20, lines 15-35),

requesting a decryption key (key) from a remote server (content provider) (col. 3, lines 45-50, col. 21, lines 20-65 and col. 22, lines 1-10).

Glover explicitly does not disclose "receiving the decryption key from the remote server at the user computing device, the decryption key itself encrypted at the remote server with a user key, the user key bonded to the user computing device by being based at least in part on one or more characteristics of the user computing device such that the user computing device can use the user key to decrypt the decryption key."

However, En-Seung clearly discloses receiving the decryption key (temporary validation key) from the remote server at the user computing device (col. 7, lines 52-61),

the decryption key itself encrypted at the remote server with a user key (user's key) (col. 6, lines 30-36), such that the user computing device can use the user key to decrypt the decryption key (col. 7, lines 6-16).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated En-Seung's invention within Glover to include receiving the decryption key from the remote server at the user computing device, the decryption key itself encrypted at the remote server with a user key, such that the user computing device can use the user key to decrypt the decryption key. One of ordinary skill in the art would have been motivated to prevent an individual from making a useful copy of the information (col. 2, lines 20-23 of Glover).

Glover and En-Seung do not disclose the user key bonded to the user computing device by being based at least in part on one or more characteristics of the user computing device.

However, Eberhard clearly discloses the user key bonded to the user computing device by being based at least in part on one or more characteristics of the user computing device (paragraph 0023).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Eberhard's invention within Glover and En-Seung to include user key bonded to the user computing device by being based at least in part on one or more characteristics of the user computing device. One of ordinary skill in the art would have been motivated to do this because the encrypted file

can only be displayed as clear text on the requesting reader (Eberhard, paragraph 0012).

Glover, En-Seung and Eberhard disclose the limitations as discussed in Claim 1 above. Glover further discloses responding to receipt of said decryption key from said remote server at the user computing device by: decrypting said media content at the user computing device using said integral decryption engine and the decryption key (col. 3, lines 45-50 and col. 21, lines 45-65).

Regarding Claim 3, Glover En-Seung and Eberhard disclose the limitations as discussed in Claim 1 above. Glover further discloses after decrypting the media content, viewing said media content by executing external viewer software linked to said file (col. 21, lines 20-60).

Regarding Claim 17, Glover En-Seung and Eberhard disclose the limitations as discussed in Claim 35 above. Glover further discloses wherein the file is executable independently of other programs and wherein requesting the decryption key and decrypting the media content are accomplished by executing the file (col. 21, lines 45-50).

Regarding Claim 20, Glover En-Seung and Eberhard disclose the limitations as discussed in Claim 2 above. Glover further discloses wherein decrypting the media

content and viewing the media content are accomplished without storing a decrypted copy of the media content locally (col. 6, lines 55-65).

Regarding Claim 25, Glover En-Seung and Eberhard disclose the limitations as discussed in Claim 1 above. Glover En-Seung and Eberhard further disclose wherein receiving the file at the user computing device comprises downloading the file using a peer to peer network from a remote computer that is different from the remote server (Eberhard, Figure 1, paragraph 0012).

Regarding Claim 34, Glover En-Seung and Eberhard disclose the limitations as discussed in Claim 1 above. En-Seung further discloses generating the user key at the user computing device (col. 6, lines 58-63).

Regarding Claim 35, Glover En-Seung and Eberhard disclose the limitations as discussed in Claim 34 above. En-Seung further discloses wherein decrypting the media content at the user computing device using the integral decryption engine and the decryption key comprises using the user key to decrypt the decryption key and to thereby obtain a decrypted decryption key (col. 16, lines 20-30).

Regarding Claim 36, Glover En-Seung and Eberhard disclose the limitations as discussed in Claim 35 above. En-Seung further discloses wherein using the user key to

decrypt the decryption key is performed without storing the decrypted decryption key in memory accessible to a user of the user computing device (col. 12, lines 22-30).

Regarding Claim 38, Glover En-Seung and Eberhard disclose the limitations as discussed in Claim 36 above. En-Seung further discloses wherein decrypting the media content and viewing the media content are accomplished without storing a decrypted copy of the media content in memory accessible to a user of the user computing device (col. 3, lines 35-50).

Regarding Claim 41, Glover En-Seung and Eberhard disclose the limitations as discussed in Claim 35 above. Glover En-Seung and Eberhard further disclose wherein receiving the file at the user computing device comprises downloading the file using a peer to peer network from a remote computer that is different from the remote server (Eberhard, Figure 1, paragraph 0012).

Regarding Claim 42, Glover En-Seung and Eberhard disclose the limitations as discussed in Claim 1 above. En-Seung further discloses wherein decrypting the media content at the user computing device using the integral decryption engine and the decryption key comprises using the user key to decrypt key and to thereby obtain a decrypted decryption key (col. 6, lines 55-65).

Regarding Claim 47, Glover, En-Seung and Eberhard disclose the limitations as discussed in Claim 1 above. Glover, En-Seung and Eberhard further disclose wherein receiving the file at the user computing device comprises receiving the file from a remote computer over a communication network (En-Seung, col. 3, lines 5-18 and col. 22, lines 10-20) that includes the remote server from which the decryption key is obtained but through a communication path that does not include the remote server from which the decryption key is received server (Eberhard, Figure 1).

Regarding Claim 48, Glover, En-Seung and Eberhard disclose the limitations as discussed in Claim 1 above. Glover, En-Seung and Eberhard further disclose sending the file from the user computing device to a second user computing device over a communication network (Figure 1 of Eberhard); upon receipt of the file at the second user computing device; sending a request, from the second user computing device to the remote server, for the decryption key; receiving the decryption key from the remote server at the second user computing device, the decryption key itself encrypted at the remote server with a second user key, the second user key bonded to the second user computing device by being based at least in part on one or more characteristics of the second user computing device such that the second user computing device can use the second user key to decrypt the decryption key; and responding the receipt of the decryption key from the remote server at the second user computing device by decrypting the media content at the second user computing device using the integral

decryption engine and the decryption key (En-Seung col. 3, lines 5-18 and col. 22, lines 10-20, col. 6, lines 30-36, col. 7, lines 6-16 and 52-61).

Regarding Claim 49, Glover, En-Seung and Eberhard disclose the limitations as discussed in Claim 48 above. En-Seung further discloses after receiving the file at the second user computing device, generating the second user key at the second user computing device (col. 6, lines 59-63).

Regarding Claim 50, Glover, En-Seung and Eberhard disclose the limitations as discussed in Claim 49 above. Glover, En-Seung and Eberhard further disclose wherein decrypting the media content at the second user computing device using the integral decryption engine and the decryption key comprises using the second user key to decrypt the decryption key and to thereby obtain a decrypted decryption key (col. 5, lines 20-25 of En-Seung).

Regarding Claim 55, Glover, En-Seung and Eberhard disclose the limitations as discussed in Claim 1 above. Glover, En-Seung and Eberhard further disclose wherein the decryption key received at the user computing device is permanent such that decrypting the media content at the user computing device using the integral decryption engine and the decryption key may be performed multiple times at the user computing device using the integral decryption engine and the same decryption key (col. 3, lines

45-50 and col. 20, lines 15-35 of Glover, col. 7, lines 52-61 of En-Seung, and paragraph 0023 of Eberhard).

4. Claims 4-6, 11, 21, 28, 31, 43-44, 51-54 and 56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Glover (U.S. Patent 6,052,780) herein referred to as Glover in view of Budge et al. (U.S. Patent 6,564,248 B1) herein referred to as Budge and in view of En-Seung et al. (U.S. Patent 6,892,306 B1) herein referred to as En-Seung and further in view of Eberhard et al. (U.S. Patent Publication 2001/001238 A1) herein referred to as Eberhard.

Regarding Claim 4, Glover discloses a method of managing distribution of proprietary electronic media, the method comprising:

receiving a single file (computer program) at a user computing device (col. 4, lines 30-35), the file comprising an integral decryption engine and encrypted media content (encrypted digital information) (col. 3, lines 45-50), but Glover explicitly does not disclose "integral media playback software."

However, Budge expressly discloses integral media playback software (col. 2, lines 25-30).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Glover's invention with Budge to provide integral media playback software. One of ordinary skill in the art would have

been motivated to allow the receiving system to view the video file without necessity of previously installing special software at the receiving system (col. 6, lines 15-20).

Glover and Budge disclose the limitations of Claim 4 above. Furthermore, Glover discloses the single file executable independently of other program to:

decrypt the media content using the integral decryption engine and a decryption key obtained separately from the file (col. 3, lines 45-50 and col. 21, lines 20-65); and Budge explicitly discloses view the media content using the integral media playback software (col. 6, lines 15-20).

Glover and Budge explicitly do not disclose "obtain the decryption key from a remote server, the decryption key itself encrypted at the remote server with a user key, the user key bonded to the user computing device by being based at least in part on one or more characteristics of the user computing device such that the user computing device can use the user key to decrypt the decryption key."

However, En-Seung clearly discloses obtain the decryption key (temporary validation key) from a remote server (service server) (col. 7, lines 52-61), the decryption key itself encrypted at the remote server with a user key (users' key) (col. 6, lines 30-36), such that the user computing device can use the user key to decrypt the decryption key (col. 7, lines 6-16).

Accordingly, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated En-Seung's invention within Glover and Budge to include obtain the decryption key from a remote server, the decryption key itself encrypted at the remote server with a user key, such that the user computing

device can use the user key to decrypt the decryption key. One of ordinary skill in the art would have been motivated to prevent an individual from making a useful copy of the information (col. 2, lines 20-23 of Glover).

Glover Budge and En-Seung do not disclose the user key bonded to the user computing device by being based at least in part on one or more characteristics of the user computing device.

However, Eberhard clearly discloses the user key bonded to the user computing device by being based at least in part on one or more characteristics of the user computing device (paragraph 0023).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Eberhard's invention with Glover, Budge and En-Seung to include user key bonded to the user computing device by being based at least in part on one or more characteristics of the user computing device. One of ordinary skill in the art would have been motivated to do this because the encrypted file can only be displayed as clear text on the requesting reader (Eberhard, paragraph 0012).

Regarding Claim 5, Glover, Budge, En-Seung and Eberhard disclose the limitations as discussed in Claim 4 above. Glover further discloses wherein downloading the single file comprises downloading said single file from a remote server via a communication network (col. 21, lines 5 and col. 22, lines 15-20).

Regarding Claim 6, Glover, Budge, En-Seung and Eberhard disclose the limitations as discussed in Claim 5 above. Glover further discloses downloading said decryption key from said remote server via said communication network (col. 21, lines 60-65 and col. 22, lines 1-10).

Regarding Claim 11, Glover, Budge, En-Seung and Eberhard disclose the limitations as discussed in Claim 6 above. Glover further discloses wherein said remote server tracks a number of decrypting key downloads relating to the single file (col. 21, lines 5-10).

Regarding Claim 21, Glover, Budge, En-Seung and Eberhard disclose the limitations as discussed in Claim 4 above. Glover further discloses wherein decrypting the media content and viewing the media content are accomplished without storing a decrypted copy of the media content locally (col. 6, lines 55-65).

Regarding on Claim 28, Glover, Budge, En-Seung and Eberhard disclose the limitations as discussed in Claim 4 above. Glover further discloses wherein the single file is executable to view the media content using the integral media playback software without storing a decrypted copy of the media content in memory accessible to a user of the user computing device (col. 20, lines 55-67).

Regarding Claim 31, Glover, Budge, En-Seung and Eberhard disclose the limitations as discussed in Claim 4 above. Glover further discloses wherein server tracks a number of decryption keys relating to the single file that have been issued by the remote server (col. 21, lines 5-10).

Regarding Claim 43, Glover, Budge, En-Seung and Eberhard disclose the limitations as discussed in Claim 4 above. En-Seung further discloses wherein execution of the single file causes the user computing device to generate the user key at the user computing device (col. 6, lines 59-63).

Regarding Claim 44, Glover, Budge, En-Seung and Eberhard disclose the limitations as discussed in Claim 43 above. En-Seung further discloses wherein execution of the single file to decrypt the media content using the integral decryption engine and the decryption key comprises using the user key to decrypt the decryption key and to thereby obtain a decrypted decryption key (col. 5, lines 20-25).

Regarding Claim 51, Glover, Budge, En-Seung and Eberhard disclose the limitations as discussed in Claim 6 above. En-Seung further discloses wherein the computer is different from the communication network from which the sinqle file is downloaded includes the remote server from which the decryption key is obtained and wherein downloadinq the single file from the computer via the communication network comprises downloadinq the sinqle file from the computer through a communication path

that does not include the remote server from which the decryption key is obtained (col. 3, lines 5-18 and col. 22, lines 10-20).

Regarding Claim 52, Glover, Budge, En-Seung and Eberhard disclose the limitations as discussed in Claim 4 above. Glover, Budge, En-Seung and Eberhard further disclose sending the file from the user computing device to a second user computing device over a communication network (Figure 1 of Eberhard); upon receipt of the file at the second user computing device; sending a request, from the second user computing device to the remote server, for the decryption key; receiving the decryption key from the remote server at the second user computing device, the decryption key itself encrypted at the remote server with a second user key, the second user key bonded to the second user computing device by being based at least in part on one or more characteristics of the second user computing device such that the second user computing device can use the second user key to decrypt the decryption key; and responding the receipt of the decryption key from the remote server at the second user computing device by decrypting the media content at the second user computing device using the integral decryption engine and the decryption key (col. 3, lines 5-18 and col. 22, lines 10-20, col. 6, lines 30-36, col. 7, lines 6-16 and 52-61).

Regarding Claim 53, Glover, Budge, En-Seung and Eberhard disclose the limitations as discussed in Claim 52 above. En-Seung further discloses after receiving

the file at the second user computing device, generating the second user key at the second user computing device (col. 6, lines 59-63).

Regarding Claim 54, Glover, Budge, En-Seung and Eberhard disclose the limitations as discussed in Claim 53 above. En-Seung further discloses wherein decrypting the media content at the second user computing device using the integral decryption engine and the decryption key comprises using the second user key to decrypt the decryption key and to thereby obtain a decrypted decryption key (col. 5, lines 20-25).

Regarding Claim 56, Glover, Budge, En-Seung and Eberhard disclose the limitations as discussed in Claim 4 above. Glover, Budge, En-Seung and Eberhard further disclose wherein the decryption key obtained at the user computing device is permanent such that subsequent executions of the single file decrypt the media content at the user computing device using the integral decryption engine and the same decryption key (col. 3, lines 45-50 and col. 20, lines 15-35 of Glover, col. 7, lines 52-61 of En-Seung, and paragraph 0023 of Eberhard).

5. Claims 2, 18 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Glover, En-Seung and Eberhard as applied to claim 1 above, and further in view of Budge et al. (U.S. Patent 6,564,248 B1) herein referred to as Budge.

Regarding Claim 2, Glover, En-Seung and Eberhard disclose the limitations as discussed in Claim 1 above. Glover further discloses after decrypting the media content (col. 3, lines 45-50), but Glover, En-Seung and Eberhard explicitly do not disclose viewing said media content by executing viewer software, the viewer software also integral with said file.

However, Budge expressly discloses viewing said media content by executing viewer software, the viewer software also integral with said file (col. 2, lines 25-30).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Budge's invention within Glover, En-Seung and Eberhard to provide viewing said media content by executing viewer software, the viewer software also integral with said file. One of ordinary skill in the art would have been motivated to allow the receiving system to view the video file without necessity of previously installing special software at the receiving system (col. 6, lines 15-20).

Regarding Claim 18, Glover, En-Seung and Eberhard disclose the limitations as discussed in Claim 17 above. Glover, En-Seung and Eberhard do not disclose wherein the file also comprises integral media player software.

However, Budge expressly discloses wherein the file also comprises integral media player software (col. 2, lines 25-30).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Budge's invention within Glover, En-Seung and Eberhard to provide wherein the file also comprises integral media player software. One of ordinary skill in the art would have been motivated to allow the receiving system to view the video file without necessity of previously installing special software at the receiving system (col. 6, lines 15-20).

Regarding Claim 20, Glover, En-Seung, Eberhard and Budge disclose the limitations as discussed in Claim 2 above. Glover further discloses wherein decrypting the media content and viewing the media content are accomplished without storing a decrypted copy of the media content locally (col. 20, lines 55-67).

6. Claim 33 is rejected under 35 U.S.C. 103(a) as being unpatentable over Glover, Budge, En-Seung, and Eberhard as applied to claim 4 above, and further in view of Wiser et al. (U.S. Patent 6,385,596 B1) herein referred to as Wiser.

Regarding Claim 33, Glover, Budge, En-Seung, and Eberhard disclose the limitations as discussed in Claim 4 above. Glover, Budge, En-Seung, and Eberhard explicitly do not disclose wherein a portion of the media content is previewable prior to decrypting the media content using the integral decryption engine and the decryption key.

However, Wiser expressly discloses a portion of the media content is previewable prior to decrypting the media content using the integral decryption engine and the decryption key (col. 3, lines 50-60).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Wiser's invention within Glover, Budge, En-Seung, and Eberhard to provide a portion of the media content is previewable prior to decrypting the media content using the integral decryption engine and the decryption key. One of ordinary skill in the art would have been motivated to allow the consumer has the opportunity to watch the portion of the video program before ordering (col. 3, lines 55-60).

7. Claims 27 and 40 is rejected under 35 U.S.C. 103(a) as being unpatentable over Glover, En-Seung and Eberhard as applied to claim 1 above, and further in view of Wiser et al. (U.S. Patent 6,385,596 B1) herein referred to as Wiser.

Regarding Claims 27 and 40, Glover, En-Seung and Eberhard disclose the limitations as discussed in Claim 4 above. Glover, En-Seung and Eberhard explicitly do not disclose wherein a portion of the media content is previewable prior to decrypting the media content using the integral decryption engine and the decryption key.

However, Wiser expressly discloses a portion of the media content is previewable prior to decrypting the media content using the integral decryption engine and the decryption key (col. 3, lines 50-60).

Accordingly, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Wiser's invention within Glover, En-Seung and Eberhard to provide a portion of the media content is previewable prior to decrypting the media content using the integral decryption engine and the decryption key. One of ordinary skill in the art would have been motivated to allow the consumer has the opportunity to watch the portion of the video program before ordering (col. 3, lines 55-60).

Contact Information

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Baotran N. To whose telephone number is 571-272-8156. The examiner can normally be reached on Monday-Friday from 8:00 to 4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

BT
07/05/2007

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100